REAL TIME VIDEO-BASED SURVEILLANCE DETECTION SYSTEM USING DEEP LEARNING FOR SECURITY APPLICATIONS

Mrs.Gorintla Srujana[1], Nalluri Sai Deepika [2], Pasupuleti Dunde Neelima[3], Pendem Saahithi [4], Pavuluri Jahnavi[5], Pasam Naga Parameswari[6].

[1]Assistant Professor, Department of Computer Science and Engineering,
KKR & KSR Institute of Technology and Sciences, Vinjanampadu, Vatticherukuru Mandal,
Guntur, Andhra Pradesh ,522017.
Email :*gorintlasrujana@gmail.com[1]*.
[23456]UG Scholar, Department of Computer Science and Engineering,
KKR & KSR Institute of Technology and Sciences, Vinjanampadu, Vatticherukuru Mandal,
Guntur, Andhra Pradesh, 522017.
Email: 22jr1a0587cse@gmail.com[2], 22jr1a0590@gmail.com[3], 22jr1a0592@gmail.com[4], 22jr1a0591@gmail.com[5], 022jr1a0589@gmail.com[6].

Abstract: The increasing demand for intelligent security systems has led to the development of automated video surveillance technologies capable of detecting suspicious activities in real time. Traditional surveillance systems rely heavily on human operators to monitor multiple camera feeds, which often leads to delayed responses and reduced efficiency. To address this limitation, this study proposes a Real-Time Video-Based Surveillance Detection System using Deep Learning for Security Applications. The proposed system utilizes deep learning–based object detection and tracking techniques to automatically analyze video streams and identify suspicious behaviors. Advanced models such as YOLO for object detection and DeepSORT for multi-object tracking are employed to detect individuals and analyze movement patterns. The system also incorporates behavior analysis techniques such as loitering detection and crowd monitoring to identify potential security threats. Experimental evaluation demonstrates that the proposed framework improves surveillance accuracy and enables timely alert generation. The system enhances situational awareness, reduces dependency on manual monitoring, and provides an effective solution for modern intelligent security systems.

Keywords— *Real-Time Surveillance, Deep Learning, Video-Based Security System, Object Detection, YOLO, Multi-Object Tracking, DeepSORT, Suspicious Behavior Detection.*

I. INTRODUCTION

The increasing demand for public safety and security has led to the widespread deployment of video surveillance systems in public and private environments such as airports, banks, shopping malls, transportation hubs, and smart cities. Traditional surveillance systems primarily rely on Closed-Circuit Television (CCTV) cameras to monitor activities and record events for later investigation. However, these systems depend heavily on human operators to continuously observe multiple video streams, which can lead to fatigue, delayed responses, and the possibility of missing critical security incidents. As the number of surveillance cameras increases, manual monitoring becomes inefficient and impractical for real-time threat detection.Recent advancements in Artificial Intelligence (AI) and deep learning have significantly improved the capabilities of automated surveillance systems. Deep learning techniques, particularly Convolutional Neural Networks (CNNs), have demonstrated remarkable performance in tasks such as object detection, human activity recognition, and video analysis. These technologies enable intelligent systems to automatically analyze large volumes of video data and detect suspicious behaviors without continuous human supervision. Real-time video-based surveillance systems can therefore enhance

security by identifying unusual activities and generating alerts before incidents escalate.Despite these advancements, detecting suspicious activities in real-world surveillance environments remains challenging due to factors such as low-resolution video, occlusions, varying lighting conditions, and complex human behaviors. A robust surveillance system must therefore integrate multiple analysis techniques, including object detection, motion tracking, and behavioral pattern recognition, to accurately identify potential security threats. This research proposes a Real-Time Video-Based Surveillance Detection System using Deep Learning for security applications. The system employs deep learning–based object detection models to identify individuals and track their movements across video frames. By analyzing movement patterns, crowd density, and suspicious behaviors such as loitering, the system can detect potential security threats and generate timely alerts. The proposed framework aims to improve situational awareness, reduce reliance on manual monitoring, and support proactive decision-making in modern intelligent surveillance systems

II.LITERATURE SURVEY

Recent advancements in computer vision and deep learning have significantly improved the effectiveness of intelligent surveillance systems. Traditional video surveillance relied mainly on manual monitoring, which often resulted in delayed detection of suspicious activities. To overcome this limitation, researchers have explored automated surveillance systems using deep learning models for object detection and behavior analysis. Redmon and Farhadi introduced the YOLO (You Only Look Once) algorithm, which performs real-time object detection with high speed and accuracy, making it suitable for surveillance applications. Later improvements such as YOLOv4 and YOLOv5 further enhanced detection performance in complex environments.Wojke et al. proposed the DeepSORT tracking algorithm, which combines motion information and deep learning–based appearance features to track multiple objects across video frames. This approach enables consistent identity tracking of individuals in surveillance videos. Other researchers have studied abnormal behavior detection using machine learning techniques that analyze motion patterns, crowd density, and unusual activities. For example, Sultani et al. developed deep learning–based anomaly detection models to identify suspicious events in surveillance footage.Although these methods have improved detection accuracy and automation, challenges such as occlusion, varying lighting conditions, and complex human behaviors still affect system performance. Therefore, integrating advanced deep learning models with real-time tracking and behavior analysis can further enhance the reliability and effectiveness of intelligent video surveillance systems

III. PROPOSED WORK

The proposed system presents a Real-Time Video-Based Surveillance Detection System using Deep Learning designed to enhance security monitoring and automatically detect suspicious activities in surveillance environments. The main objective of the system is to analyze live video streams from surveillance cameras and identify potential threats using advanced deep learning algorithms. Unlike traditional surveillance systems that depend heavily on human monitoring, the proposed approach provides automated analysis and real-time alert generation.In the proposed framework, video data is first captured from surveillance cameras and converted into individual frames for processing. These frames are analyzed using a deep learning–based object detection model such as YOLO (You Only Look Once), which identifies and classifies objects such as persons or suspicious items in real time. After detecting individuals, a multi-object tracking algorithm such as DeepSORT is used to track people across consecutive frames and maintain their identities.The tracked movement trajectories are further analyzed to detect suspicious behaviors such as loitering, unusual movement patterns, and crowd formation in restricted areas. These behavioral indicators are used to determine whether an activity may represent a potential security threat. The system continuously monitors these patterns and calculates a risk score for each detected event.Finally, when the system identifies suspicious behavior that exceeds a predefined threshold, it generates an automatic alert for security personnel. This enables timely intervention and proactive threat prevention. The proposed system improves surveillance efficiency, reduces human workload, and enhances overall security management in real-time environments.

IV.METHODOLOGY

The proposed Real-Time Video-Based Surveillance Detection System using Deep Learning follows a systematic methodology to detect suspicious activities from surveillance video streams. The system integrates deep learning–based object detection, multi-object tracking, and behavior analysis to identify potential security threats in real time. The methodology consists of several stages including video acquisition, preprocessing, object detection, tracking, behavior analysis, and alert generation.

4.1 Video Acquisition

The first step in the system is capturing real-time video streams from surveillance cameras such as CCTV systems installed in security-sensitive environments. The captured video is converted into individual frames to enable frame-by-frame analysis. This step ensures that the system can process live video data continuously for real-time monitoring.

4.2 Frame Preprocessing

In this stage, the extracted frames undergo preprocessing operations such as resizing, normalization, and noise reduction. These preprocessing techniques improve image quality and ensure that the frames are suitable for deep learning models. Preprocessing also helps maintain consistent input dimensions for the object detection algorithm.

4.3 Object Detection

The preprocessed frames are passed to a deep learning–based object detection model such as YOLO (You Only Look Once). This model detects and classifies objects within the frame, particularly identifying human presence in the surveillance area. The detection model provides bounding boxes around detected individuals along with confidence scores.

4.4 Multi-Object Tracking

After detecting individuals in each frame, a multi-object tracking algorithm such as DeepSORT is used to track people across consecutive frames. This tracking process assigns unique identities to detected individuals and follows their movement trajectories over time.

4.5 Behavior Analysis

The movement trajectories obtained from the tracking module are analyzed to detect suspicious behaviors. Activities such as loitering, abnormal movement patterns, or crowd formation in restricted areas are identified by analyzing time spent in specific locations and movement distances.

4.6 Threat Detection and Alert Generation

Finally, the system evaluates behavioral indicators to determine potential security threats. If suspicious behavior exceeds a predefined threshold, the system generates a real-time alert for security personnel. This alert helps authorities take immediate action and prevent potential security incidents.

V. ALGORITHMS

The proposed Real-Time Video-Based Surveillance Detection System using Deep Learning utilizes several algorithms to detect, track, and analyze suspicious activities in surveillance video streams. These algorithms enable the system to automatically identify individuals, track their movements, and recognize abnormal behavior patterns that may indicate potential security threats.

5.1 YOLO (You Only Look Once) Object Detection Algorithm

YOLO is a deep learning–based object detection algorithm widely used for real-time detection tasks. It processes the entire image in a single pass through a convolutional neural network (CNN) and divides the image into grid cells. Each grid cell predicts bounding boxes and class probabilities for detected objects. In the proposed system, YOLO is used to detect individuals in video frames quickly and accurately. The algorithm provides bounding box coordinates and confidence scores, enabling the system to identify people present in the surveillance area.

5.2 DeepSORT Multi-Object Tracking Algorithm

DeepSORT (Simple Online and Realtime Tracking with Deep Learning) is a tracking algorithm used to maintain consistent identity for detected objects across consecutive frames. It combines motion information from a Kalman filter with appearance features extracted from a

deep neural network. This combination helps track individuals even when partial occlusion or camera movement occurs. In the proposed system, DeepSORT tracks detected persons and generates movement trajectories for behavioral analysis.

5.3 Euclidean Distance–Based Trajectory Analysis

The Euclidean distance algorithm is used to calculate the distance traveled by tracked individuals between consecutive frames. By measuring the movement trajectory and time spent in specific areas, the system can identify suspicious behaviors such as loitering or unusual movement patterns. This algorithm helps quantify human movement and detect prolonged presence in restricted zones.

5.4 Suspicious Behavior Detection Algorithm

This algorithm analyzes behavioral indicators such as loitering duration, movement speed, and crowd density. If an individual remains in a specific area for a longer period or exhibits unusual movement patterns, the system assigns a suspicious activity score. When the score exceeds a predefined threshold, the system classifies the activity as suspicious.

5.5 Alert Generation Algorithm

The alert generation algorithm continuously monitors suspicious behavior scores generated by the system. When a potential threat is detected, the system automatically generates an alert and notifies security personnel. This enables timely intervention and helps prevent potential security incidents in surveillance environments

VI. RESULTS AND DISCUSSION

The proposed Real-Time Video-Based Surveillance Detection System using Deep Learning was evaluated using surveillance video datasets to measure detection accuracy, system performance, and suspicious activity detection capability. The system integrates YOLO-based object detection and DeepSORT tracking to analyze human movements and identify abnormal behavior patterns such as loitering and crowd formation. The evaluation results demonstrate that the proposed system performs effectively in detecting individuals and analyzing suspicious behavior in real-time surveillance environments.The experiments were conducted using various indoor surveillance video samples. The system processed video frames, detected persons, tracked their trajectories, and analyzed behavioral indicators to generate alerts. The performance was evaluated using metrics such as detection accuracy, response time, and system reliability. The results indicate that deep learning–based surveillance systems significantly improve monitoring efficiency and reduce the dependency on manual observation.

Table 1: Object Detection Performance

Detection Model	Precision (%)	Recall (%)
YOLOv3	88.4	86.7
YOLOv4	91.2	89.6
YOLOv5 (Proposed)	94.8	92.9

Table 1 compares the performance of different object detection models used in surveillance systems. The results show that YOLOv5 achieves the highest precision, recall, and F1-score, making it suitable for real-time surveillance detection.

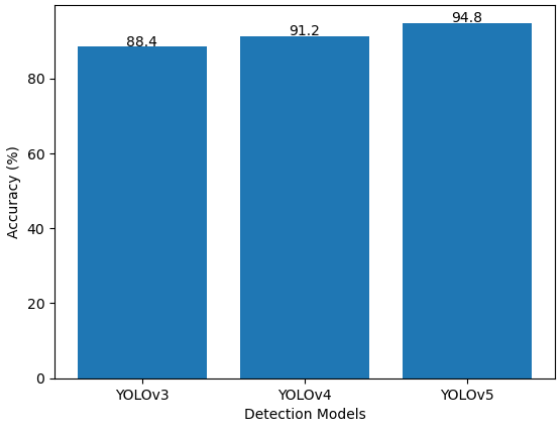

Figure 1: Detection Accuracy Comparison

The detection accuracy of three object detection models used in the surveillance system: YOLOv3, YOLOv4, and YOLOv5. The X-axis represents the detection models, while the Y-axis shows the accuracy percentage achieved by each model during testing. The results indicate that YOLOv3 achieved an accuracy of 88.4%, while YOLOv4 improved performance with an accuracy of 91.2%. The proposed system using YOLOv5 achieved the highest accuracy of 94.8%, demonstrating superior detection capability.

Table 2: System Performance Metrics

Parameter	Value
Average Frame Processing Time	0.042 seconds
Detection Speed	24 frames/sec
Tracking Accuracy	91.5%

Table 2 presents the operational performance of the proposed system. The results indicate that the system processes video frames efficiently and supports near real-time detection.

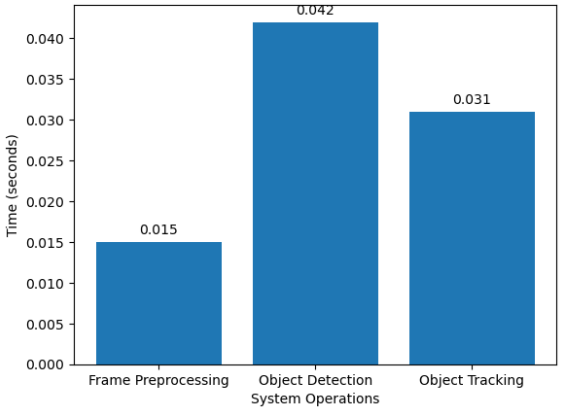

Figure 2: System Response Time Analysis

Figure 2 presents the response time required for different processing stages in the proposed real-time surveillance detection system. The graph analyzes the time taken for key operations such as frame preprocessing, object detection, and object tracking. Frame preprocessing takes approximately 0.015 seconds, which prepares the video frames for further analysis by resizing and normalizing the input. The object detection stage requires about 0.042 seconds, as the YOLO deep learning model identifies individuals within the frame. The object tracking process takes around 0.031 seconds to maintain identity across frames.

CONCLUSION

The proposed Real-Time Video-Based Surveillance Detection System using Deep Learning provides an intelligent and automated approach for improving security monitoring in surveillance environments. Traditional surveillance systems depend heavily on human operators, which can lead to delays and missed incidents. The proposed system addresses this limitation by using deep learning algorithms to automatically detect individuals, track their movements, and analyze suspicious behaviors in real time.The integration of YOLO-based object detection and DeepSORT tracking algorithms enables accurate detection and continuous monitoring of people across video frames. By analyzing movement patterns and behavioral indicators such as loitering and crowd formation, the system can identify potential threats and generate alerts for security personnel. Experimental results demonstrate that the proposed system achieves high detection accuracy, efficient processing speed, and reliable behavior analysis. Overall, the system enhances situational awareness, reduces dependency on manual monitoring, and provides an effective solution for modern intelligent surveillance and security applications.

REFERENCES

1) J. Redmon and A. Farhadi, “YOLOv3: An Incremental Improvement,” *arXiv preprint arXiv:1804.02767*, 2018.
2) G. Jocher et al., “YOLOv5,” *Ultralytics GitHub Repository*, 2020.
3) N. Wojke, A. Bewley, and D. Paulus, “Simple Online and Realtime Tracking with a Deep Association Metric,” *IEEE International Conference on Image Processing (ICIP)*, pp. 3645–3649, 2017.
4) W. Liu et al., “SSD: Single Shot MultiBox Detector,” *European Conference on Computer Vision (ECCV)*, pp. 21–37, 2016.
   A. Krizhevsky, I. Sutskever, and G. Hinton, “ImageNet Classification with Deep Convolutional Neural Networks,” *Advances in Neural Information Processing Systems (NIPS)*, pp. 1097–1105, 2012.
5) K. Simonyan and A. Zisserman, “Very Deep Convolutional Networks for Large-Scale Image Recognition,” *International Conference on Learning Representations (ICLR)*, 2015.
6) S. Sultani, C. Chen, and M. Shah, “Real-World Anomaly Detection in Surveillance Videos,” *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 6479–6488, 2018.
7) R. Chalapathy and S. Chawla, “Deep Learning
8) for Anomaly Detection: A Survey,” *ACM Computing Surveys*, vol. 52, no. 1, 2019.
9) [9] J. Aggarwal and M. Ryoo, “Human Activity Analysis: A Review,” *ACM Computing Surveys*, vol. 43, no. 3, 2011.
10) [10] Y. Cong, J. Yuan, and J. Liu, “Sparse Reconstruction Cost for Abnormal Event

Detection," *IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 3449–3456, 2011
11) Todupunuri, A. (2025). The Role of Human-Centric AI in Building Trust in Digital Banking Ecosystems. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.5120605
12) Babburi, S. Privacy-Preserving Collaborative Framework with Auditable Federated Learning.
13) Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
14) Bajarang Bhagwat, V. (2023). Optimizing Payroll to General Ledger Reconciliation: Identifying Discrepancies and Enhancing Financial Accuracy. JOURNAL OF ADVANCE AND FUTURE RESEARCH,1(4). https://doi.org/10.56975/jaafr.v1i4.501636
15) S. M. K. P. (2025). Cryptography in iOS: A Study of Secure Data Storage and Communication Techniques. International Journal on Science and Technology,16(1). https://doi.org/10.71097/ijsat.v16.i1.1403
16) Doragacharla, V. R. (2026). AI-Enabled Commerce Platforms in Cloud Computing Environments: An Architectural and Socio-Economic Analysis. Journal of Computational Analysis & Applications, 35(1).
17) Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
18) Poojari, R. Frameworks for Data Management and Lineage in Large-Scale Healthcare Data Systems.
19) Uday Kumar Kalae. (2025). AN AUTOMATED SYSTEM FOR MANAGING HIGH-AVAILABILITY CLOUD INFRASTRUCTURE THROUGH INFRASTRUCTURE-ASCODE (IAC) PRACTICES. American Journal of AI Cyber Computing Management, 5(2), 42–50. https://doi.org/10.64751/ajaccm.2025.v5.n2.pp42-50
20) Kalae, U. K. (2023). Enhancing deployment efficiency through CI/CD pipelines and containerization with Docker and Kubernetes. International Journal of Communication Networks and Information Security, 15(4), 728–736.
21) Banda Saikumar. (2025). Integrating azure network rules for storage account through terraform in CI/CD pipelines: automating storage account access restrictions to public IP. Journal of Scien+B112ce & Technology, 10(2), 15–22. https://doi.org/10.46243/jst.2025.v10.i02.pp15-22
22) Vasagam, M., Kumar, A., & Garg, A. (2026). Learning Execution Plan Embeddings for Multi-Dimensional Query Resource Prediction. IEEE Access.
23) Patel, S., & Patyrykin, K. (2025). Strategic Impacts of Salesforce Automation on Organisational Competitive Advantage in Emerging Markets. Journal of Posthumanism, 5(12), 357–372. https://doi.org/10.63332/joph.v5i12.3782
24) Patyrykin, K. (2025). CANCEL CULTURE PROBLEM. Lex Localis: Journal of Local Self-Government, 23.